Michigan Cyber Initiative News

February 2013, Issue 12

Articles of Interest

California AG Issues First-in-U.S. Mobile App Privacy Guidelines
California continues to toughen its stance on mobile privacy as the state's attorney general issues privacy protection guidance. — Read this article here.

Chrome Clickjacking Vulnerability Could Expose User Information on Google, Amazon
Vulnerability could make it possible for attackers to collect users' e-mail addresses, first and last names and other information. — Read this article here.

UPnP Networking Flaw Puts Millions of PCs at Risk
Security researchers say danger stems from widely used technology found in routers and other standard networking equipment.— Read this article here.

Government Has a New Cyber Security Plan; PC Hardware to Come with Statutory Warning
In light of the rising instances of cyber crime in the country, the government of India reportedly has some changes lined up. — Read this article here.

Google's Password Proposal: One Ring to Rule Them All
Google engineers float the idea of supplementing passwords with hardware you wear, carry, or slip on-to a finger. — Read this article here.

Georgia Tech's 'Titan' Malware Intelligence System Offers Threat Sharing, Collaboration Tools
A new malware intelligence system is helping government agencies and private companies. — Read this article here.

Did You Know?

Around this time of year, many IT security companies provide a threat report summarizing the previous year's events and offer their predictions for the upcoming year.

Some resources have not published their reports as of yet so continue looking for more as 2013 moves forward.

For now, you can view 2012 threat reports and/or 2013 predictions from:

- McAfee 2013 Threats Predictions
- Sophos Security Threat Report 2013
- Kaspersky Security Trends in 2012; Predicts Core Threat for 2013

What Are Your 2013 Security Goals?

Governor Snyder and the State of Michigan have many goals this year around security. Many of them include being proactive rather than reactive.

With several groups having made threats against specific organizations and with the breaches of 2012, it is ever more important to be proactive.

Our goals include spreading awareness and working on building partnerships for a stronger defense to the many security issues we face everyday.

Part of our plan to be proactive is to look into the security breaches of 2012 to ensure that the same doesn't happen here.

Be sure to take a look at Michigan's Cyber Initiative document.

Do You Want People to Really Act on Security Messages?

By: Dan Lohrmann

Just when I thought I was turning the corner on Internet security awareness and cyber safety, along comes an eye-opening situation that hits so close to home that I am forced to rethink the road ahead - again.

The key questions that I'm reassessing as we head into 2013: Am I saying the right things about cybersecurity? Are the most important messages getting through? Are people (even the ones who know and like us) hearing what we say? Am I genuinely listening to them – first? Allow me to explain with a personal story.

It all started when Katherine was in our kitchen trying to help her friend Carli with her new iPhone 5 that she also got for Christmas. Carli's WiFi was not working properly.

Katherine to Carli: "You turned off the 4-digit security PIN that I configured for you!" (Dad, who was in an adjacent room, suddenly became interested in this unexpected security conversation and put the magazine down.)

Carli to Katherine: "The screen lock is such a pain. And if I lose my iPhone, whoever finds it won't be able to call me and return it."

Katherine to Carli: "Yes, they can. There's an app to find it. I showed you…."

Carli to Katherine: "But…, Mrs. Lohrmann, help – you told me you haven't enabled a PIN for your iPhone either…. "

Priscilla to Carli and Katherine: "You're right. I haven't enabled the PIN…. yet. I'm not sure if it's really needed or not. But don't tell your dad, I'm still deciding…." (Dad, who is listening in the other room, now enters the kitchen.)

Dad to all: "What did you just say?"

After that conversation, I've started to reconsidered the effectiveness of what I personally say to family members about personal online security as well as whether our enterprise messages are working (or not) for state employees.

Not that we haven't been through this discussion before. Priscilla and I talk about online safety quite often as it relates to our children. We agree on the vast majority of steps we take with security on PCs, Internet access controls and filtering. It's just that the conversation and examples keep changing as technology evolves and the kids get older.

And my thoughts often move towards work, where the same concerns and questions apply. Yes, we've already reinvented awareness training for employees in the past year to focus on the new online challenges and mobile situations. We did listen to employees and heard that the old training was out of date, boring and irrelevant. But now I'm worried that we're still not doing enough. Or, perhaps, we're falling behind in our messaging – again.

What Do We Do – and Say?

In response, we offer revised policies, compliance regulations, new awareness training and new approaches like testing whether employees click on bad links. Every little bit helps, but can we do more?

My gut tells me that I need to start by looking in the mirror. Lead by my example. So what are my 2013 security resolutions?

- To keep watching and analyzing our state government culture
- To learn the new ways our people are using technology
- To listen to the business more
- To keep refining the security and privacy messages we are delivering to employees
- To help people understand the impact of their actions
- To offer enabling security that truly helps

To read the full article, click here.

Excerpted by permission from Lohrmann on Cybersecurity, www.govtech.com, January 7, 2013.